



#4

AT-0024US

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Takayuki SATO

Appln. No. 10/063,933

Group Art Unit: 2131

Filed: May 28, 2002

Examiner: Unknown

Confirmation No. 7803

For: COMMUNICATION SYSTEM, INTERCONNECTING DEVICE AND PROGRAM
FOR AUTHENTICATING A USER OF A COMMUNICATION NETWORK

SUBMISSION OF PRIORITY DOCUMENT(S)

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir,

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims
the right of priority based on the following application(s):

<u>Country</u>	<u>Application No.</u>	<u>Filed</u>
Japan	2002-41305	February 19, 2002

A certified copy of the above-noted application(s) is (are) attached hereto.

Respectfully submitted,

Karan Singh

Registration No. 38698

RYUKA IP LAW FIRM

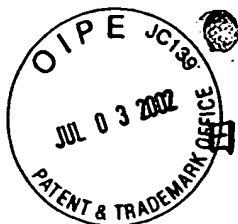
6th Floor, Toshin Building, 1-24-12,

Shinjuku, Shinjuku-ku, Tokyo, Japan

Telephone: +81-3-5366-7377

Facsimile: +81-3-5366-7288

Date: July 1, 2002



本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 2月19日

出 願 番 号

Application Number:

特願2002-041305

[ST.10/C]:

[JP2002-041305]

出 願 人

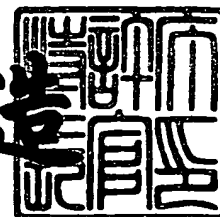
Applicant(s):

アライドテレシス株式会社

2002年 3月 5日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2002-3013766

【書類名】 特許願

【整理番号】 IP2202001

【提出日】 平成14年 2月19日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/56

【発明者】

 【住所又は居所】 東京都品川区西五反田 7-22-17 TOCビル ア
 ライドテレシス株式会社内

 【氏名】 佐藤 貴之

【特許出願人】

 【識別番号】 396008347

 【氏名又は名称】 アライドテレシス株式会社

【代理人】

 【識別番号】 100104156

 【弁理士】

 【氏名又は名称】 龍華 明裕

 【電話番号】 (03)5366-7377

【手数料の表示】

 【予納台帳番号】 053394

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信システム、中継機器、及びプログラム

【特許請求の範囲】

【請求項 1】 第 1 ネットワークと第 2 ネットワークとを接続する通信システムであって、

前記第 1 ネットワークの第 1 通信機器に接続された第 1 中継機器と、

前記第 1 中継機器及び前記第 2 ネットワークの第 2 通信機器に接続され、前記第 1 通信機器と前記第 2 通信機器との通信を許可するか否かを制御する第 2 中継機器と、

前記第 2 中継機器に前記第 1 通信機器のユーザを認証させるための認証情報を格納する記録機器と

を備え、

前記第 1 中継機器は、

前記第 2 中継機器に前記第 1 通信機器のユーザを認証させるための認証情報を、前記記録機器から取得する取得部と、

前記取得部が取得した前記認証情報を前記第 2 中継機器に送信する送信部とを有することを特徴とする通信システム。

【請求項 2】 前記第 2 中継機器は、

前記認証情報を前記第 1 中継機器から受信する受信部と、

前記受信部が受信した前記認証情報を認証する認証部と、

前記認証部による認証が成立した場合に、前記第 1 通信機器と前記第 2 通信機器との通信を許可するように前記第 2 中継機器を設定する設定部とを有することを特徴とする請求項 1 に記載の通信システム。

【請求項 3】 前記第 1 中継機器において、

前記取得部は、前記記録機器から帯域幅を示す帯域幅情報をさらに取得し、

前記送信部は、前記取得部が取得した前記帯域幅情報を前記第 2 中継機器にさらに送信し、

前記第 2 中継機器において、

前記受信部は、前記帯域幅情報を前記第 1 中継機器からさらに受信し、

前記設定部は、前記受信部が受信した前記帯域幅情報に基づいて、前記第1通信機器と前記第2通信機器との通信の帯域幅をさらに設定することを特徴とする請求項2に記載の通信システム。

【請求項4】 第1ネットワークの第1通信機器と第2ネットワークの第2通信機器との通信を可能にすべく、前記第1ネットワークと前記第2ネットワークとを接続する中継機器であって、

前記第1通信機器と前記第2通信機器との通信を許可するか否かを制御する認証装置に前記第1通信機器のユーザを認証させるための認証情報を、当該中継機器の外部の記録機器から取得する取得部と、

前記取得部が取得した前記認証情報を前記認証装置に送信する送信部とを備えることを特徴とする中継機器。

【請求項5】 前記記録機器は、前記認証情報を格納する不揮発性メモリであり、

前記取得部は、前記不揮発性メモリから前記認証情報を読み出す読出部を有することを特徴とする請求項4に記載の中継機器。

【請求項6】 前記記録機器は、前記認証情報を格納し、当該中継機器と無線通信を行う無線通信端末であり、

前記取得部は、前記無線通信端末から前記認証情報を無線通信により受信する無線受信部を有することを特徴とする請求項4に記載の中継機器。

【請求項7】 前記取得部は、前記記録機器から前記認証装置の識別情報をさらに取得し、

前記送信部は、前記取得部が取得した前記認証情報を、前記取得部が取得した前記識別情報で識別される前記認証装置に送信することを特徴とする請求項4に記載の中継機器。

【請求項8】 前記第1通信機器と前記第2通信機器との通信の帯域幅を設定する設定部をさらに備え、

前記取得部は、前記記録機器から帯域幅を示す帯域幅情報をさらに取得し、

前記設定部は、前記取得部が取得した前記帯域幅情報に基づいて、前記第1通信機器と前記第2通信機器との通信の帯域幅を設定することを特徴とする請求項

4に記載の中継機器。

【請求項9】 前記取得部が暗号化された前記認証情報を取得した場合に、暗号化された前記認証情報を復号化する復号部をさらに備えることを特徴とする請求項4に記載の中継機器。

【請求項10】 前記認証装置に前記ユーザを認証させるか否かを判断する判断部をさらに備え、

前記送信部は、前記判断部が前記認証装置に前記ユーザを認証させると判断した場合に、前記取得部が取得した前記認証情報を前記認証装置に送信することを特徴とする請求項4に記載の中継機器。

【請求項11】 前記判断部は、前記第1通信機器に電源が投入された場合に、前記認証装置に前記ユーザを認証させると判断することを特徴とする請求項10に記載の中継機器。

【請求項12】 前記判断部は、当該中継機器に電源が投入された場合に、前記認証装置に前記ユーザを認証させると判断することを特徴とする請求項10に記載の中継機器。

【請求項13】 第1ネットワークの第1通信機器と第2ネットワークの第2通信機器との通信を可能にすべく、前記第1ネットワークと前記第2ネットワークとを接続する中継機器用のプログラムであって、前記中継機器を、

前記第1通信機器と前記第2通信機器との通信を許可するか否かを制御する認証装置に前記第1通信機器のユーザを認証させるための認証情報を、当該中継機器の外部の記録機器から取得する取得手段、

及び前記取得手段が取得した前記認証情報を前記認証装置に送信する送信手段として機能させるためのプログラム。

【請求項14】 前記第1通信機器と前記第2通信機器との通信の帯域幅を設定する設定手段としてさらに機能させ、

前記取得手段は、前記記録機器から帯域幅を示す帯域幅情報をさらに取得し、

前記設定手段は、前記取得部が取得した前記帯域幅情報に基づいて、前記第1通信機器と前記第2通信機器との通信の帯域幅を設定することを特徴とする請求項13に記載のプログラム。

【請求項15】 前記取得部が暗号化された前記認証情報を取得した場合に、暗号化された前記認証情報を復号化する復号手段としてさらに機能させることを特徴とする請求項13に記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信システム、中継機器、及びプログラムに関する。特に本発明は、任意のユーザによる通信回線の不正使用を防止する通信システム、中継機器、及びプログラムに関する。

【0002】

【従来の技術】

近年の家庭におけるインターネット利用の普及に伴い、音楽、画像データ、及び動画データ等の大量のデータを、インターネットを介して配信する高速回線の実現が期待されている。この要求を受けて、ADSL (Asymmetric Digital Subscriber Line)、FTTH (Fiber To The Home) 等の普及化が進められており、PPPoE (Point to Point over Ethernet) 接続に対応したルータを介してインターネットに接続するユーザが増加している。

【0003】

【発明が解決しようとする課題】

従来のPPPoE接続に対応したルータは、一般的にユーザによって設定されたユーザ名及びパスワードを保存し、ユーザの指示に従ってユーザ名及びパスワードをインターネットサービスプロバイダの認証装置に送信することにより、インターネットへの接続が許可される。したがって、従来のルータは、任意のユーザの指示に従ってインターネットに接続することができるため、任意のユーザによって通信回線を不正に使用される恐れがあるという問題がある。

【0004】

そこで本発明は、上記の課題を解決することのできる通信システム、中継機器、及びプログラムを提供することを目的とする。この目的は特許請求の範囲にお

ける独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【0005】

【課題を解決するための手段】

即ち、本発明の第1の形態によると、第1ネットワークと第2ネットワークとを接続する通信システムであって、第1ネットワークの第1通信機器に接続された第1中継機器と、第1中継機器及び第2ネットワークの第2通信機器に接続され、第1通信機器と第2通信機器との通信を許可するか否かを制御する第2中継機器と、第2中継機器に第1通信機器のユーザを認証させるための認証情報を格納する記録機器とを備え、第1中継機器は、第2中継機器に第1通信機器のユーザを認証させるための認証情報を、記録機器から取得する取得部と、取得部が取得した認証情報を第2中継機器に送信する送信部とを有する。

【0006】

第2中継機器は、認証情報を第1中継機器から受信する受信部と、受信部が受信した認証情報を認証する認証部と、認証部による認証が成立した場合に、第1通信機器と第2通信機器との通信を許可するように第2中継機器を設定する設定部とを有してもよい。

【0007】

第1中継機器において、取得部は、記録機器から帯域幅を示す帯域幅情報をさらに取得し、送信部は、取得部が取得した帯域幅情報を第2中継機器にさらに送信し、第2中継機器において、受信部は、帯域幅情報を第1中継機器からさらに受信し、設定部は、受信部が受信した帯域幅情報に基づいて、第1通信機器と第2通信機器との通信に使用可能な帯域幅をさらに設定してもよい。

【0008】

本発明の第2の形態によると、第1ネットワークの第1通信機器と第2ネットワークの第2通信機器との通信を可能にすべく、第1ネットワークと第2ネットワークとを接続する中継機器であって、第1通信機器と第2通信機器との通信を許可するか否かを制御する認証装置に第1通信機器のユーザを認証させるための認証情報を、当該中継機器の外部の記録機器から取得する取得部と、取得部が取

得した認証情報を認証装置に送信する送信部とを備えてもよい。

【0009】

記録機器は、認証情報を格納する不揮発性メモリであり、取得部は、不揮発性メモリから認証情報を読み出す読出部を有してもよい。記録機器は、認証情報を格納し、当該中継機器と無線通信を行う無線通信端末であり、取得部は、無線通信端末から認証情報を無線通信により受信する無線受信部を有してもよい。

【0010】

取得部は、記録機器から認証装置の識別情報をさらに取得し、送信部は、取得部が取得した認証情報を、取得部が取得した識別情報で識別される認証装置に送信してもよい。

【0011】

第1通信機器と第2通信機器との通信の帯域幅を設定する設定部をさらに備え、取得部は、記録機器から帯域幅を示す帯域幅情報をさらに取得し、設定部は、取得部が取得した帯域幅情報に基づいて、第1通信機器と第2通信機器との通信に使用可能な帯域幅を設定してもよい。

【0012】

取得部が暗号化された認証情報を取得した場合に、暗号化された認証情報を復号化する復号部をさらに備えてもよい。

【0013】

認証装置にユーザを認証させるか否かを判断する判断部をさらに備え、送信部は、判断部が認証装置にユーザを認証させると判断した場合に、取得部が取得した認証情報を認証装置に送信してもよい。

【0014】

判断部は、第1通信機器に電源が投入された場合に、認証装置にユーザを認証させると判断してもよい。判断部は、当該中継機器に電源が投入された場合に、認証装置にユーザを認証させると判断してもよい。

【0015】

本発明の第3の形態によると、第1ネットワークの第1通信機器と第2ネットワークの第2通信機器との通信を可能にすべく、第1ネットワークと第2ネット

ワークとを接続する中継機器用のプログラムであって、中継機器を、第1通信機器と第2通信機器との通信を許可するか否かを制御する認証装置に第1通信機器のユーザを認証させるための認証情報を、当該中継機器の外部の記録機器から取得する取得手段、及び取得手段が取得した認証情報を認証装置に送信する送信手段として機能させる。

【0016】

第1通信機器と第2通信機器との通信の帯域幅を設定する設定手段としてさらに機能させ、取得手段は、記録機器から帯域幅を示す帯域幅情報をさらに取得し、設定手段は、取得部が取得した帯域幅情報に基づいて、第1通信機器と第2通信機器との通信の帯域幅を設定してもよい。

【0017】

取得部が暗号化された認証情報を取得した場合に、暗号化された認証情報を復号化する復号手段としてさらに機能させてもよい。

【0018】

なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【0019】

【発明の実施の形態】

以下、発明の実施形態を通じて本発明を説明するが、実施形態はクレームにかかる発明を限定するものではなく、また実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【0020】

図1は、本発明の一実施形態に係る通信システム100の構成の一例を示す。本実施形態に係る通信システム100は、中継機器10a及び10bと、記録機器15a及び15bと、パーソナルコンピュータ(PC)20a、22a、20b、及び22bと、中継機器40と、インターネット網50と、Webサーバ60と、メールサーバ62とを備える。中継機器10aは、PC20a及び22aと、中継機器40を接続する。中継機器10bは、PC20b及び22bと、中継機器40を接続する。中継機器40は、中継機器10a及び10bと、インタ

ーネット網50とを接続する。

【0021】

PC20a及び22bは、LAN30aを構築し、PC20b及び22bは、LAN30bを構築する。LAN30a及び30bは、本発明に係る第1ネットワークの一例である。また、インターネット網50は、本発明に係る第2ネットワークの一例である。また、PC20a、22a、20b、及び22bは、本発明に係る第1通信機器の一例である。また、Webサーバ60及びメールサーバ62は、本発明に係る第2通信機器の一例である。また、中継機器40は、本発明に係る認証装置の一例である。

【0022】

記録機器15aは、中継機器40に中継機器10aのユーザ（即ちPC20a及び／又は22aのユーザ）を認証させるための認証情報を格納する。そして、記録機器15aは、中継機器10aに認証情報を提供する。また、記録機器15bは、中継機器40に中継機器10b（即ちPC20b及び／又は22bのユーザ）のユーザを認証させるための認証情報を格納する。そして、記録機器15bは、中継機器40に認証情報を提供する。記録機器15a及び15bは、ICカード、ミニチュアカード、フロッピーディスク等の不揮発性メモリであってもよいし、Bluetooth、IrDA等の無線通信を行う無線通信端末であってもよい。また記録器器15a及び15bは、暗号化された認証情報を格納することが望ましい。

【0023】

中継機器10aは、中継機器40に中継機器10aのユーザを認証させるための認証情報を記録機器15aから取得する。そして、中継機器10aは、LAN30aとインターネット網50とを接続するために、ユーザの指示に従って中継機器40に認証情報を送信する。また、中継機器10bは、中継機器40に中継機器10bのユーザを認証させるための認証情報を記録機器15bから取得する。そして、中継機器10bは、LAN30bとインターネット網50とを接続するために、ユーザの指示に従って中継機器40に認証情報を送信する。例えば、中継機器10a及び10bがPPPoE接続により中継機器40に接続する形態

では、中継機器10a及び10bは、認証情報としてユーザ名及びパスワードを記録機器15a又は15bから取得し、中継機器40に送信する。また、中継機器10a及び10bがダイヤルアップ接続により中継機器40に接続する形態では、中継機器10a及び10bは、認証情報として接続先電話番号、ユーザ名、及びパスワードを記憶機器15a又は15bから取得し、中継機器40に送信する。

【0024】

中継機器40は、中継機器10a及び10bと、インターネット網50とを接続するか否かを制御する。即ち、中継機器40は、PC20a、22a、20b、及び22bと、Webサーバ60及びメールサーバ62との通信を許可するか否かを制御する。

【0025】

中継機器40は、中継機器10a又は10bから受信した認証情報を認証する。そして、中継機器40は、中継機器10aから受信した認証情報の認証が成立した場合に、LAN30aとインターネット網50との通信を可能に設定する。これにより、LAN30aのPC20a及び22aは、インターネット網50に接続することができ、PC20a及び22aのユーザは、Webサーバ60及びメールサーバ62を利用することができる。また、中継機器40は、中継機器10bから受信した認証情報の認証が成立した場合に、LAN30bとインターネット網50との通信を可能にする。これにより、LAN30bのPC20b及び22bは、インターネット網50に接続することができ、PC20b及び22bのユーザは、Webサーバ60及びメールサーバ62を利用することができる。

【0026】

上述の説明において、中継機器40は、中継機器10a及び10bから受信した認証情報を認証したが、中継機器40に接続された外部の認証装置に認証処理を行わせてもよい。さらに、中継機器40と外部の認証装置とは、直接接続されて通信してもよいし、インターネット網50を介して接続されて通信してもよい。

【0027】

中継機器40を管理するインターネットプロバイダは、中継機器10aと記録機器15a、又は中継機器10b及び記録機器15bを、通信回線の契約を行ったユーザに提供する。記録機器15aは、インターネットプロバイダによって暗号化された認証情報を格納し、中継機器10aは、記録機器15aに格納された認証情報を復号化する復号鍵を有する。また、記録機器15bは、インターネットプロバイダによって暗号化された認証情報を格納し、中継機器10bは、記録機器15bに格納された認証情報を復号化する復号鍵を有する。

【0028】

これにより、記録機器15aを所有するユーザのみが中継機器10aを使用してインターネット網50に接続できる。また、記録機器15bを所有するユーザのみが中継機器10bを使用してインターネット網50に接続できる。即ち、PC20a又は22aのユーザは、中継機器10aを介してインターネット網50に接続するための鍵として、中継機器10aのユーザの認証情報が格納された記録機器15aを所持する。そして、中継機器10aに記録機器15aが格納する認証情報を取得させることによって、ユーザはPC20a又は22aを用いてインターネット網50を利用できる。また、PC20b又は22bのユーザは、中継機器10bを介してインターネット網50に接続するための鍵として、中継機器10bのユーザの認証情報が格納された記録機器15bを所持する。そして、中継機器10bに記録機器15bが格納する認証情報を取得させることによって、ユーザはPC20b又は22bを用いてインターネット網50を利用できる。また、記録機器15a及び15bが暗号化された認証情報を格納することにより、ユーザの認証情報の漏洩を防ぐことができる。

【0029】

本実施形態に係る通信システム100によれば、記録機器15aを所持するユーザのみが中継機器10aを用いてインターネット網50を利用することができるので、記録機器15aを所持するユーザ（即ち通信回線の契約者である中継機器10aのユーザ）以外の任意のユーザによる通信回線の不正使用を防止できる。同様に、記録機器15bを所持するユーザのみが中継機器10bを用いてインターネット網50を利用することができるので、記録機器15bを所持するユー

ザ（即ち通信回線の契約者である中継機器 10b のユーザ）以外の任意のユーザによる通信回線の不正使用を防止できる。

【0030】

図2は、本実施形態に係る中継機器 10a の構成の第1の例を示す。なお、中継機器 10b は、中継機器 10a と同様の構成を有しており、以下において、代表して中継機器 10a を用いて説明する。

【0031】

本実施形態の第1の例に係る中継機器 10a は、中継機器 40 に中継機器 10a のユーザを認証させるための認証情報を記録機器から取得する取得部の一例である読出部 102 と、暗号化された認証情報を復号化する復号部 104 と、中継機器 10a の通信設定を行う設定部 106 と、中継機器 40 とデータの送受信を行う外側送受信部 108 と、PC 20a 及び 22a とデータの送受信を行う内側送受信部 110 と、中継機器 40 に中継機器 10a のユーザを認証させるか否かを判断する判断部 112 とを備える。

【0032】

まず、読出部 102 は、中継機器 10a のユーザによって挿入された、中継機器 10a のユーザの認証情報を格納する IC カード、ミニチュアカード、フロッピーディスク等の不揮発性メモリである記録機器 15a を保持する。そして、読出部 102 は、不揮発性メモリである記録機器 15a から認証情報を読み出す。そして、復号部 104 は、読出部 102 が読み出した認証情報が暗号化されている場合、読出部 102 が読み出した暗号化された認証情報を復号化する。そして、外側送受信部 108 は、復号部 104 が復号化した認証情報を中継機器 40 に送信する。

【0033】

判断部 112 は、中継機器 40 に中継機器 10a のユーザを認証させるか否かを判断する。即ち、判断部 112 は、外側送受信部 108 に認証情報を送信させるか否かを判断する。具体的には、判断部 112 は、内側送受信部 110 に接続された PC 20a 又は 22a に電源が投入されたか否かを検出し、PC 20a 又は 22a に電源が投入されたことを検知した場合に、中継機器 40 に中継機器 1

0 a のユーザを認証させると判断してもよい。また、判断部 112 は、中継機器 10 a に電源が投入されたか否かを検出し、中継機器 10 a に電源が投入されたことを検知した場合に、中継機器 40 に中継機器 10 a のユーザを認証させると判断してもよい。また、判断部 112 は、内側送受信部 110 が PC 20 a 又は 22 a からパケットを受信したか否かを検出し、内側送受信部 110 が PC 20 a 又は 22 a からパケットを受信した場合に、中継機器 40 に中継機器 10 a のユーザを認証させると判断してもよい。そして、外側送受信部 108 は、判断部 112 が中継機器 40 に中継機器 10 a のユーザを認証させると判断した場合に、読出部 102 が不揮発性メモリである記録機器 15 a から読み出した認証情報を中継機器 40 に送信してもよい。

【0034】

また、読出部 102 は、不揮発性メモリである記録機器 15 a から、中継機器 40 の識別情報をさらに読み出してもよい。そして、外側送受信部 108 は、記録機器 15 から読み出した認証情報を、記録機器 15 a から読み出した識別情報で識別される中継機器 40 に送信してもよい。これにより、1つの中継機器 10 a を用いて、容易に複数の中継機器 40（即ち複数のインターネットプロバイダ）のいずれかに接続することができ、通信回線の用途に応じてインターネットプロバイダを変更することが可能になる。

【0035】

また、読出部 102 は、不揮発性メモリである記録機器 15 a から、中継機器 10 a が中継機器 40 において通信可能な帯域幅を示す帯域幅情報をさらに読み出してもよい。そして、設定部 106 は、読出部 102 が記録機器 15 a から読み出した帯域幅情報に基づいて、PC 20 a 及び 22 a と、中継機器 40 との通信の帯域幅、即ち PC 20 a 及び 22 a と、Web サーバ 60 及びメールサーバ 62 との通信に使用可能な帯域幅を設定してもよい。具体的には、設定部 106 は、中継機器 40 と外側送受信部 108 との通信の帯域幅を制限してもよいし、PC 20 a 及び 22 a と内側送受信部 110 との通信の帯域幅を制限してもよい。これにより、中継機器 40 の管理者（即ちインターネットプロバイダ）は、中継機器 10 a のユーザが使用可能な通信の帯域幅を容易に設定することができる。

。また、外側送受信部108は、読出部102が記録機器15aから読み出した帯域幅情報を中継機器40aに送信してもよい。

【0036】

図3は、本実施形態に係る中継機器10aの構成の第2の例を示す。図2に示した第1の例の中継機器10aと同様の構成要素は、図2と同様の符号を付す。また、図2に示した第1の例の中継機器10aと同様の構成及び動作についての説明は一部省略し、特に図2に示した第1の例の中継機器10aと異なる構成及び動作について説明する。

【0037】

本実施形態の第2の例に係る中継機器10aは、第1の例の中継機器10aの読出部102に換えて、無線通信部103を備える。無線通信部103は、中継機器10aのユーザの認証情報を格納する無線通信端末である記録機器15aから無線通信により認証情報を受信する。また、無線通信部103は、無線通信端末である記録機器15aから、中継機器40の識別情報をさらに読み出してもよい。無線通信部103は、無線通信端末である記録機器15aから、中継機器40の識別情報をさらに読み出してもよい。

【0038】

図4は、本実施形態に係る中継機器40の構成の一例を示す。本実施形態に係る中継機器40は、中継機器10aのユーザを認証する認証部204と、中継機器10aとデータの送受信を行う内側送受信部206と、インターネット網50に対してデータの送受信を行う外側送受信部200と、中継機器40の通信設定を行う設定部202とを備える。

【0039】

まず、内側送受信部206は、中継機器10aからユーザの認証情報を受信する。そして、認証部204は、内側送受信部206が中継機器10aから受信した認証情報を認証する。そして、設定部202は、認証部204による認証が成立した場合に、中継機器10aとインターネット網50との通信を許可するように中継機器40を設定する。

【0040】

また、内側送受信部206は、中継機器10aから帯域幅情報をさらに受信してもよい。そして、設定部202は、内側送受信部206が受信した帯域幅情報に基づいて、中継機器10aとインターネット網との通信の帯域幅、即ちPC20a及び22aと、Webサーバ60及びメールサーバ62との通信の帯域幅を設定してもよい。具体的には、設定部202は、内側送受信部206の中継機器10aが接続されたポートにおける通信の帯域幅を制限してもよい。これにより、中継機器40の管理者（即ちインターネットプロバイダ）は、中継機器10aのユーザが使用する通信の帯域幅を容易に設定することができる。

【0041】

図5は、本実施形態に係る通信システム100の動作フローの一例を示す。まず、中継機器10aにおいて、図2における読出部102、又は図3における無線通信部103は、暗号化された認証情報及び帯域幅情報を記録機器15aから取得する（S100）。そして、復号部104は、記録機器15aから取得した認証情報を復号化する（S102）。そして、判断部112は、PC20a又は22aに電源が投入されたか監視する（S104）。そして、PC20a又は22aが稼働している場合に、外側送受信部108は、認証情報を中継機器40に送信する（S106）。

【0042】

次に、中継機器40において、内側送受信部206は、中継機器10aが送信した認証情報を受信する（S200）。そして、認証部204は、内側送受信部206が受信した認証情報を認証する（S202）。そして、認証部206による認証が成立しなかった場合（S203-N）、中継機器40は、中継機器10aとインターネット網50との通信を許可せずに、通信システム100の動作フローは終了する。また、S203において認証部206による認証が成立した場合（S203-Y）、設定部202は、中継機器10aとインターネット網50との通信を許可するように中継機器40を設定する（S204）。そして、内側送受信部206は、認証が成立したことを示す情報を中継機器10aに送信して通知する（S205）。

【0043】

次に、中継機器10aにおいて、外側送受信部108は、帯域幅情報を中継機器に送信する(S108)。そして中継機器40において、内側送受信部206は、中継機器10aが送信した帯域幅情報を受信する(S206)。そして、設定部202は、内側送受信部206が受信した帯域幅情報に基づいて、中継機器10aとインターネット網50との通信の帯域幅を設定する(S208)。そして、PC20a及び22aは、インターネット網50を介して、Webサーバ60及びメールサーバ62と通信できる。以上で、通信システム100の動作フローは終了する。

【0044】

図6は、本実施形態に係るPC20aのハードウェア構成の一例を示す。PC20aは、CPU700と、ROM702と、RAM704と、通信インタフェース706と、ハードディスクドライブ708と、データベースインタフェース710と、フロッピーディスクドライブ712と、CD-ROMドライブ714とを備える。CPU700は、ROM702及びRAM704に格納されたプログラムに基づいて動作し、各部の制御を行う。通信インタフェース706は、コンピュータネットワークを介して中継機器10aと通信する。データベースインタフェース710は、データベースへのデータの書込、及びデータベースの内容の更新を行う。

【0045】

フロッピーディスクドライブ712は、フロッピーディスク720からデータ又はプログラムを読み取り通信インタフェース706に提供する。CD-ROMドライブ714は、CD-ROM722からデータ又はプログラムを読み取り通信インタフェース706に提供する。通信インタフェース706は、フロッピーディスクドライブ712又はCD-ROMドライブ714から提供されたデータ又はプログラムを中継機器10aに送信する。データベースインタフェース710は、各種データベース724と接続してデータを送受信する。

【0046】

中継機器10aに提供されるプログラムは、フロッピーディスク720又はCD-ROM722等の記録媒体に格納されて利用者によって提供される。記録媒

体に格納されたプログラムは圧縮されていても非圧縮であってもよい。プログラムは記録媒体から読み出され、通信インタフェース706を介して、中継機器10aにインストールされ、中継機器10aにおいて実行される。

【0047】

記録媒体に格納されて提供されるプログラム、即ち中継機器10aにインストールされるプログラムは、中継機器10aを、読出手段、無線通信手段、復号手段、設定手段、外側送受信手段、内側送受信手段、判断手段として機能させる。各手段の機能は、図1から図5において説明した中継機器10aにおける、対応する部材の動作と同一であるから、説明を省略する。

【0048】

図6に示した、記録媒体の一例としてのフロッピーディスク720又はCD-ROM722には、本出願で説明した全ての実施形態における中継機器10aの動作の一部又は全ての機能を格納することができる。

【0049】

これらのプログラムは記録媒体から直接中継機器10aによって読み出されて実行されても、中継機器10aにインストールされた後に中継機器10aにおいて実行されてもよい。更に、上記プログラムは単一の記録媒体に格納されても複数の記録媒体に格納されてもよい。又、符号化した形態で格納されていてもよい。

【0050】

記録媒体としては、フロッピーディスク、CD-ROMの他にも、DVD、PD等の光学記録媒体、MD等の光磁気記録媒体、テープ媒体、磁気記録媒体、ICカードやミニチュアカードなどの半導体メモリ等を用いることができる。また、専用通信ネットワークやインターネットに接続されたサーバシステムに設けたハードディスク又はRAM等の格納装置を記録媒体として使用し、通信網を介してプログラムを中継機器10aに提供してもよい。

【0051】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施形態に記載の範囲には限定されない。上記実施形態に、多様な変更または改良

を加えることができる。そのような変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【 0 0 5 2 】

【発明の効果】

上記説明から明らかなように、本発明によれば、任意のユーザによる通信回線の不正使用を防止する通信システムを提供することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係る通信システム 1 0 0 の構成図である。

【図 2】

本実施形態に係る中継機器 1 0 a の構成図の第 1 の例である。

【図 3】

本実施形態に係る中継機器 1 0 a の構成図の第 2 の例である。

【図 4】

本実施形態に係る中継機器 4 0 の構成図である。

【図 5】

本実施形態に係る通信システム 1 0 0 の動作フローである。

【図 6】

本実施形態に係る P C 2 0 a のハードウェア構成図である。

【符号の説明】

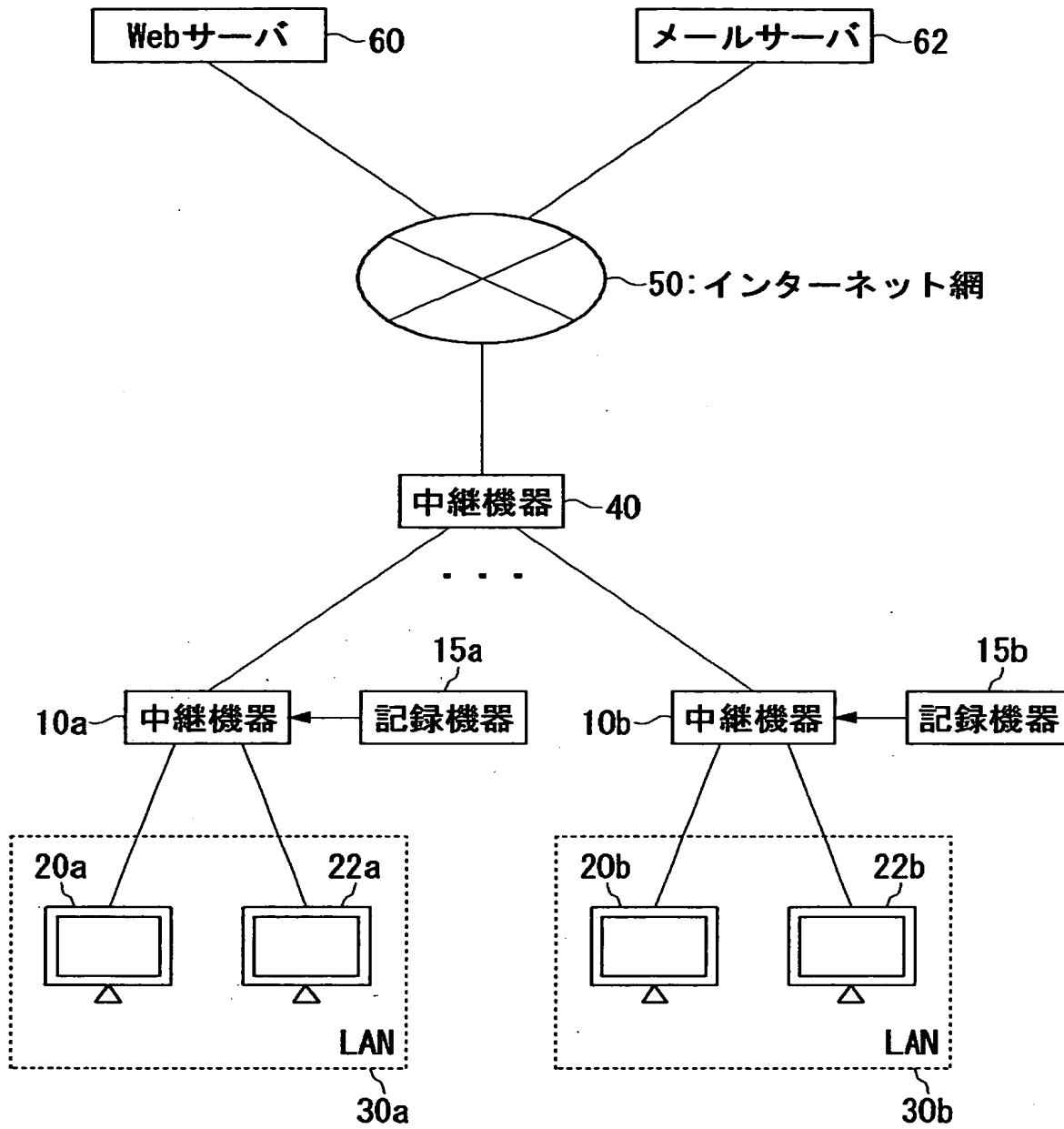
- 1 0 a、1 0 b 中継機器
- 1 5 a、1 5 b 記録機器
- 2 0 a、2 0 b、2 2 a、2 2 b P C
- 3 0 a、3 0 b L A N
- 4 0 中継機器
- 5 0 インターネット網
- 6 0 W e b サーバ
- 6 2 メールサーバ
- 1 0 0 通信システム

- 102 読出部
- 103 無線通信部
- 104 復号部
- 106 設定部
- 108 外側送受信部
- 110 内側送受信部
- 112 判断部
- 200 外側送受信部
- 202 設定部
- 204 認証部
- 206 内側送受信部
- 700 CPU
- 702 ROM
- 704 RAM
- 706 通信インタフェース
- 708 ハードディスクドライブ
- 710 データベースインタフェース
- 712 フロッピーディスクドライブ
- 714 CD-ROMドライブ
- 720 フロッピーディスク
- 722 CD-ROM
- 724 各種データベース

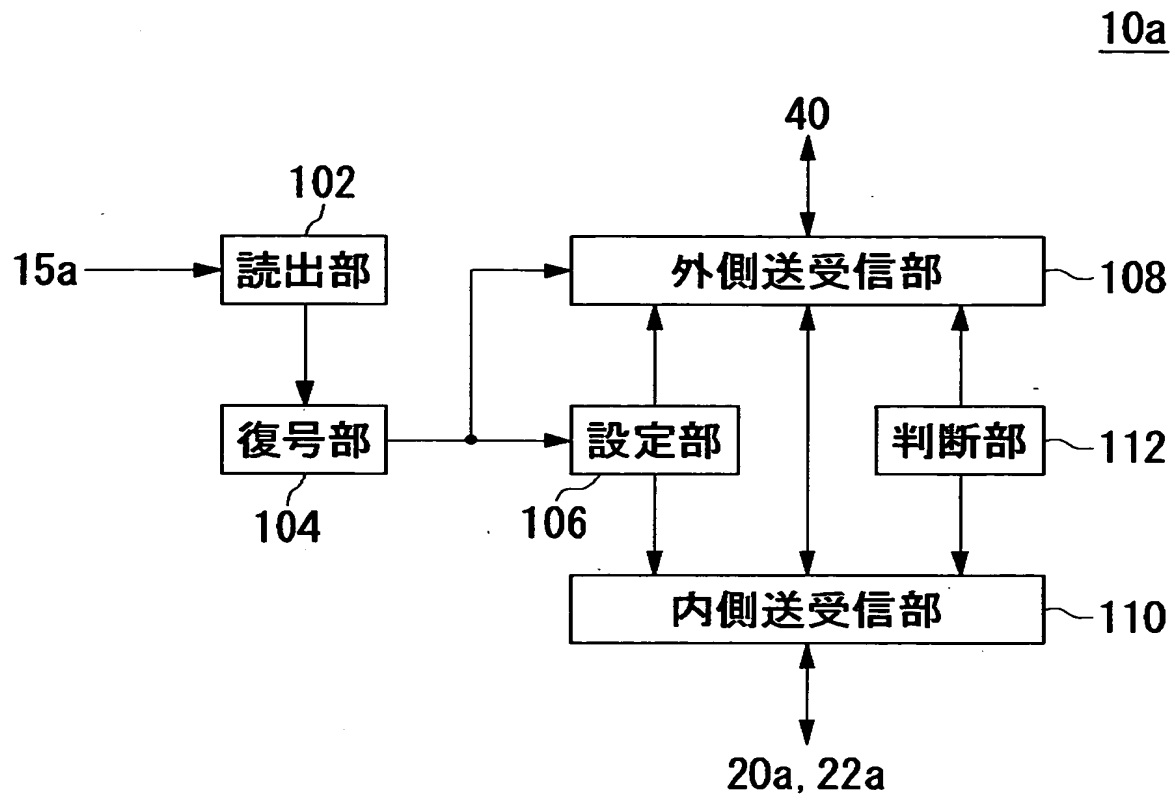
【書類名】 図面

【図 1】

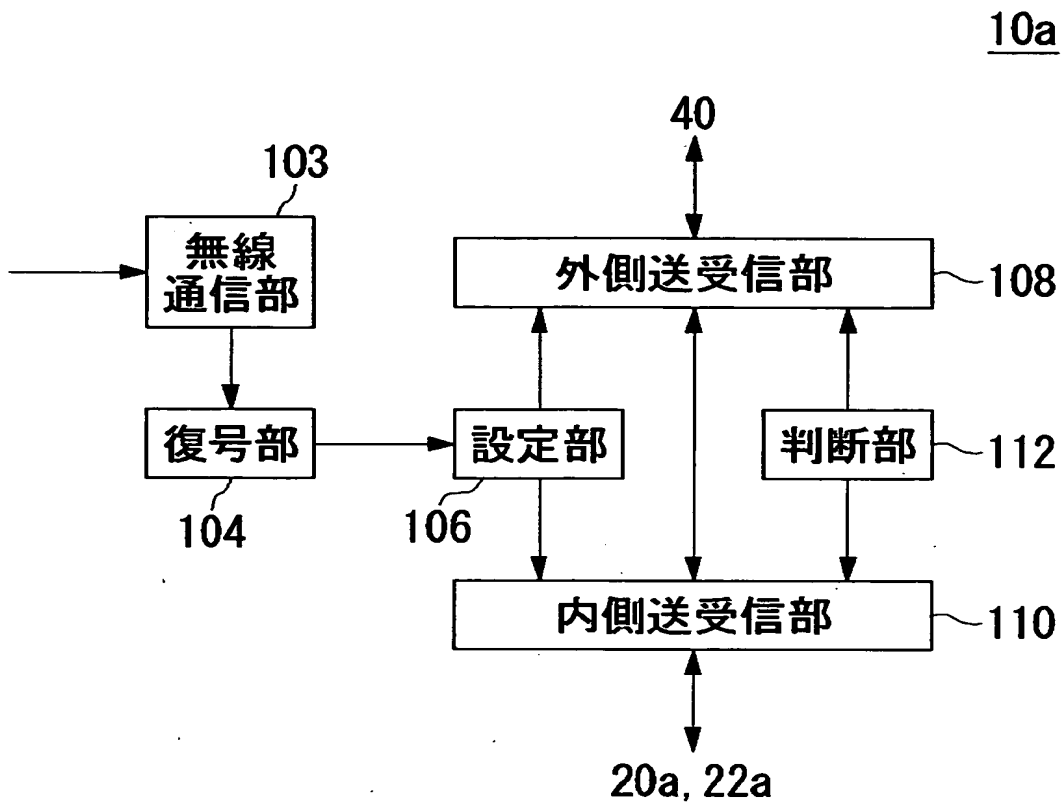
100



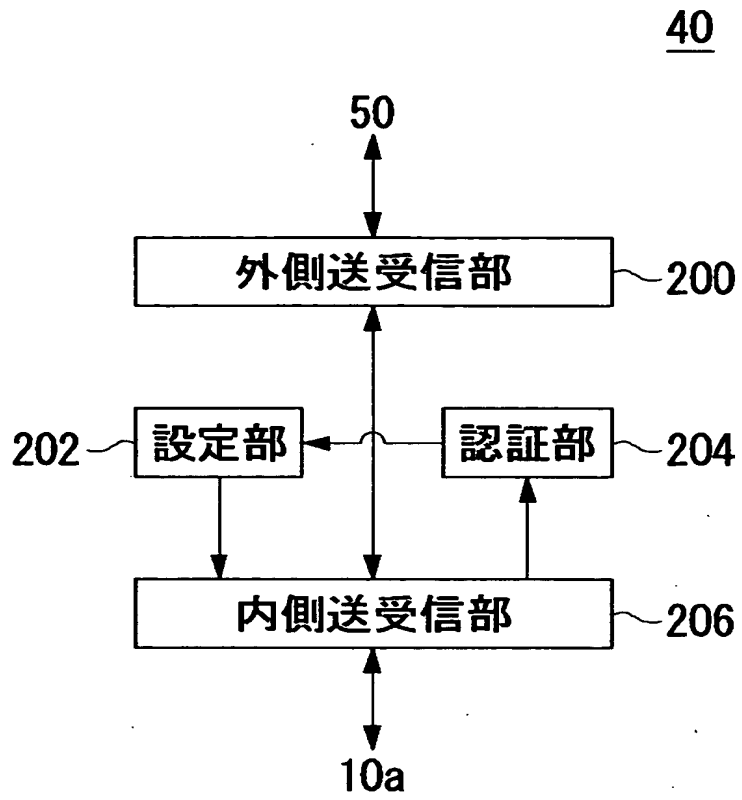
【図 2】



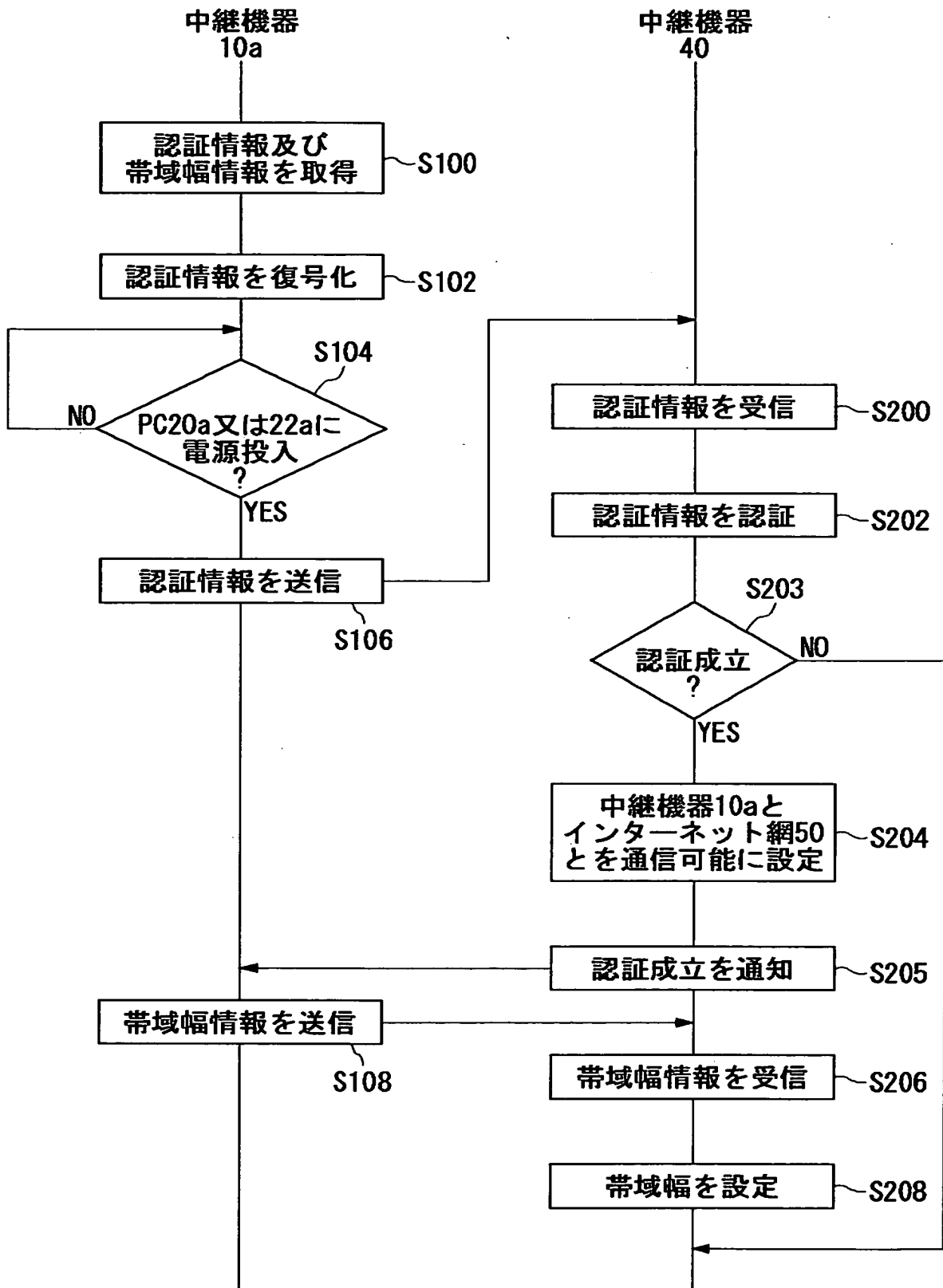
【図3】



【図 4】

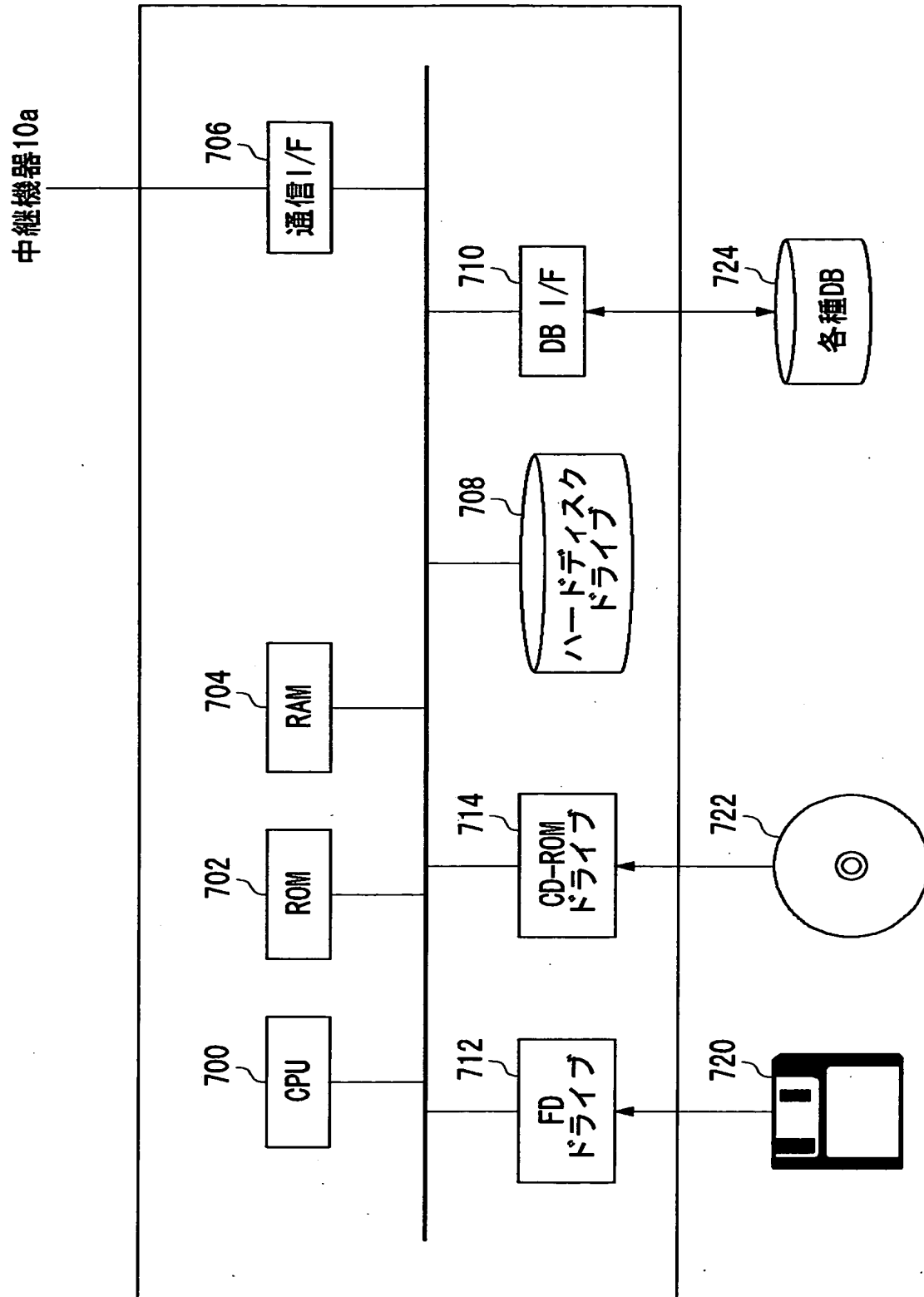


【図 5】



【図 6】

20a



【書類名】 要約書

【要約】

【課題】 任意のユーザによる通信回線の不正使用を防止する通信システムを提供することができる。

【解決手段】 本発明に係る通信システムは、第 1 ネットワークの第 1 通信機器に接続された第 1 中継機器と、第 1 中継機器及び第 2 ネットワークの第 2 通信機器に接続され、第 1 通信機器と第 2 通信機器との通信を許可するか否かを制御する第 2 中継機器と、第 2 中継機器に第 1 通信機器のユーザを認証させるための認証情報を格納する記録機器とを備える。第 1 中継機器は、第 2 中継機器に第 1 中継機器のユーザを認証させるための認証情報を、記録機器から取得する取得部と、取得部が取得した認証情報を第 2 中継機器に送信する送信部とを有する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [396008347]

1. 変更年月日	2000年10月24日
[変更理由]	住所変更
住 所	東京都品川区西五反田7-22-17 TOCビル
氏 名	アライドテレシス株式会社